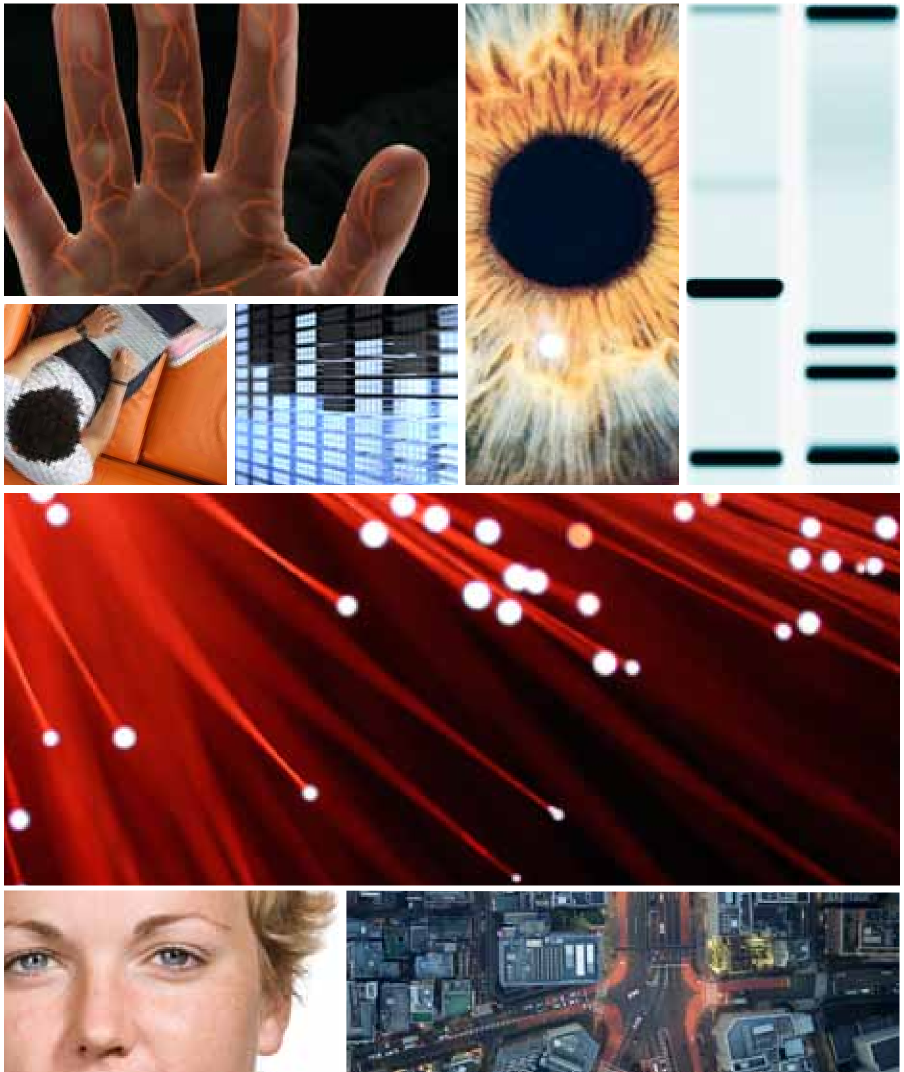
Making **Web 2.0** Work

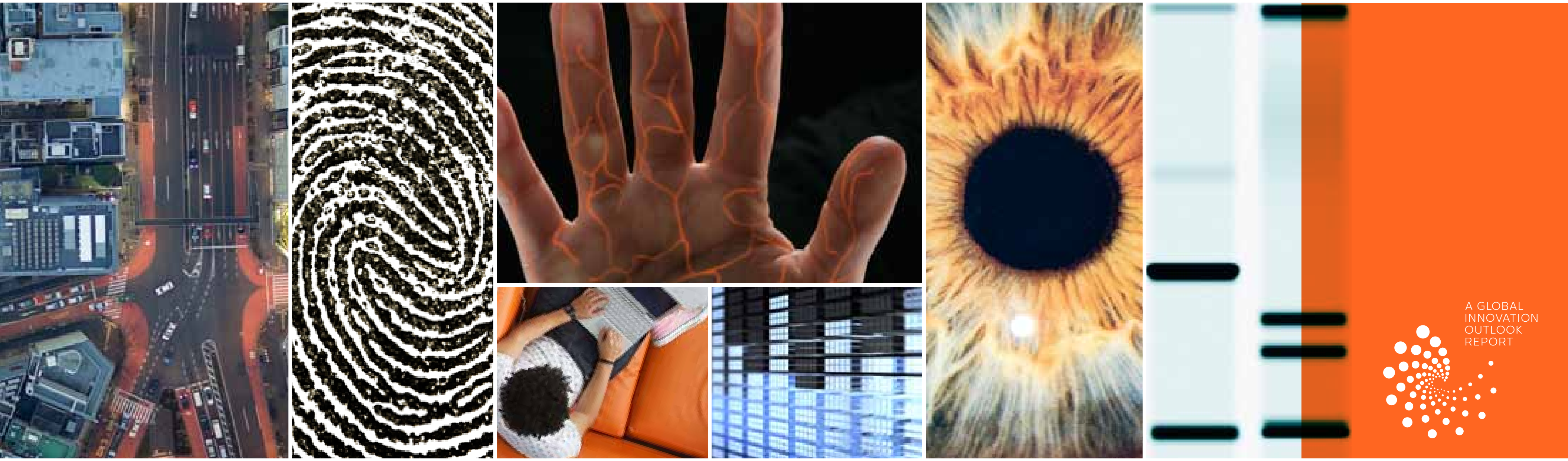


A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work



A GLOBAL
INNOVATION
OUTLOOK
REPORT

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

Making Web 2.0 Work

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

A GLOBAL
INNOVATION
OUTLOOK
REPORT

A GLOBAL
INNOVATION
OUTLOOK
REPORT

Making Web 2.0 Work

Balancing the security risks and business rewards of the interactive Web

About 20 years ago, the world was introduced to an extraordinary new medium of communication called the World Wide Web. Over the ensuing years, as adoption spread, the Web quickly and radically revolutionized the way we live and work. It introduced a new and powerful medium of social, political, and economic transaction.

Before the world could catch its collective breath from this change, Web 2.0 added a new level of interactivity to the medium. This ability to openly exchange information—to buy and sell, to consume and create—gave rise to an explosion of social and economic creativity: Web-based communities; blogs; wikis; online auctions; social-networking sites; and video-sharing sites.

Web 2.0 exponentially increased the transactional nature of the Web, and forever changed the way people express themselves, conduct business, learn about different subjects, shop, form communities, collaborate, and share their personal information.

But the embrace of Web 2.0 has also introduced serious questions about the inherent risks associated with the use of these tools. For example, what are the expectations of privacy on Web 2.0 sites? Which types of personal and work information are safe to disclose? How can consumers protect themselves against identity theft, cybercrime, and abusive marketing? When is online surveillance appropriate? What role should traditional regulatory and law enforcement organizations play? And what are the guidelines for use of Web 2.0 in the workplace?

This report is based on a survey developed and conducted by the Ponemon Institute and IBM's Global Innovation Outlook. The survey was given to more than 3,000 consumers around the world in an effort to discern the awareness of these issues among users of Web 2.0 applications and to identify the steps that businesses can take to protect themselves and their employees from the associated risks. In learning more about what security and privacy factors increase or decrease use of Web 2.0, both at home and in the workplace, developers of Web 2.0 applications can more proactively address security concerns, increasing the usage and usefulness of their sites. And employers can craft policies on Web 2.0 use that both increase the value to the company and limit risk.

Among the conclusions drawn from this report:

> Geography and culture play important roles in determining risk tolerance for Web 2.0 applications, and must be taken into account when crafting usage guidelines. This is especially true for global employers.

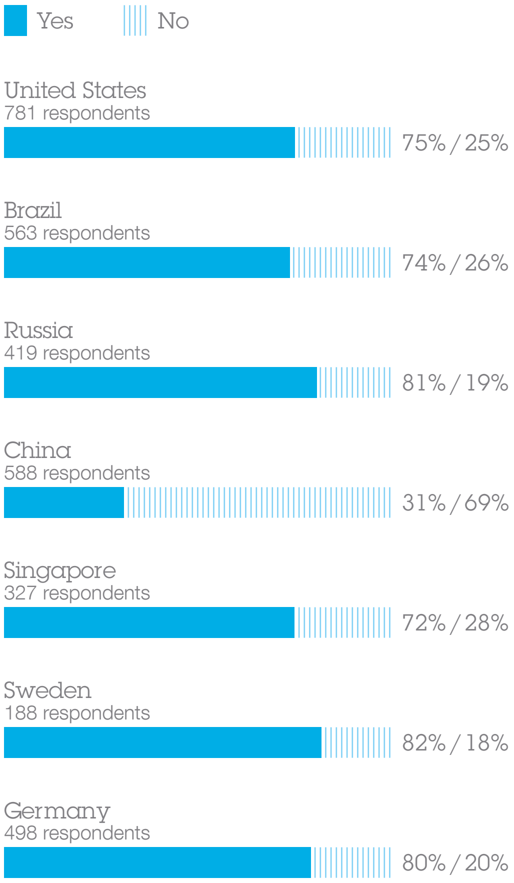
> The nature of Web 2.0 content, and its perceived benefit to the end user, greatly affects a user's willingness to assume security risks.

> There is an inherent distrust of traditional forms of regulation or law enforcement among Web 2.0 users, making attempts to artificially control or restrict use among employees likely to backfire.

> Transparent privacy policies and the ability to control one's own privacy and security settings greatly increase use of Web 2.0.

> Employers can leverage the naturally cautious instincts of Web 2.0 users and allow employees to develop their own usage policies and guidelines.

Do you use social networks, social messaging, blogs, wikis or other Web 2.0 tools on the Internet?

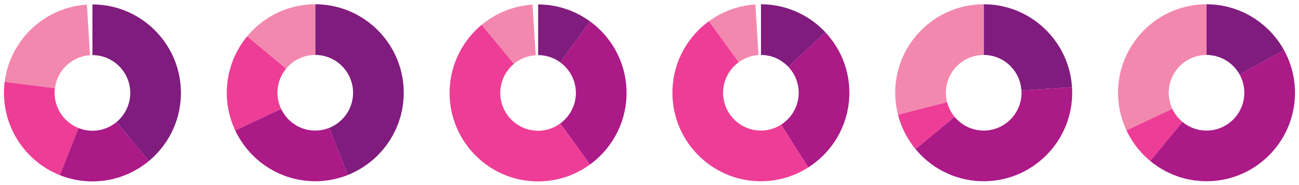


About the Survey

The survey was conceived and conducted through a collaborative effort between IBM's Global Innovation Outlook and the Ponemon Institute. It was taken by 3,364 consumers in seven different countries around the world, including the United States, Brazil, Russia, China, Singapore, Sweden, and Germany.

Respondents were asked a series of questions about their use of social networks, social messaging, blogs, wikis, and other Web 2.0 tools. The purpose was to gain an understanding of what security and privacy factors increase and decrease use of Web 2.0 applications; what users value the most about the applications; and what users are most willing to share online.

Why would you participate in Web 2.0 applications?



■ The benefits from participating outweighs any privacy or security risk

■ I benefit from exchanging information about myself with other like-minded community members

■ I believe the security of the Web 2.0 application is adequate in protecting my personal information

■ I am aware of potential dangers and willing to take steps to protect myself

□ Other

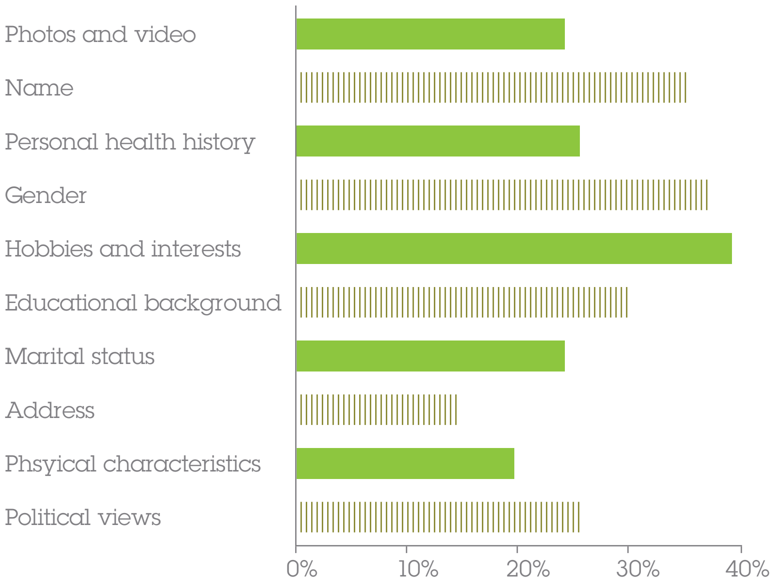
Brazil	Russia	China	Singapore	Sweden	Germany
39%	44%	10%	13%	24%	17%
17%	24%	30%	28%	40%	44%
21%	18%	49%	49%	7%	7%
22%	15%	10%	9%	30%	33%
1%	0%	1%	1%	0%	0%

The survey reveals that, in general, positive reasons for using Web 2.0 applications include: responsibility for protecting members comes from the online communities themselves and the individuals that belong to them; the amount of personal information required to belong is limited and at the discretion of users; the anonymity of users is optional; and the site provides access to quality and important information.

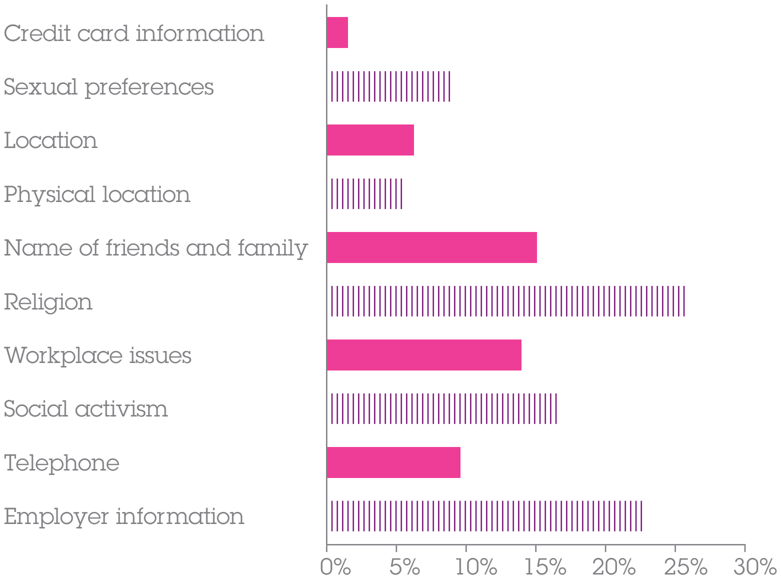
In contrast, reasons for not using Web 2.0 are: regulations and protection of members is the responsibility of the government; behavior can be monitored by law enforcement; users are asked to provide information about their credit card, location, sensitive health issues (i.e. addictions), names, and sexual preferences.

Taken together, the responses to the survey tell the story of the compromises Web 2.0 users are willing to accept in order to reap the benefits of these applications. These tradeoffs, and the point at which users are no longer willing to accept the inherent risks of Web 2.0 services, is a moving target, shifting over time as new services are introduced and social norms evolve. But at any point in time, that breaking point can be measured.

Data types users are most willing to share in Web 2.0 environments.



Data types users are least willing to share in Web 2.0 environment.



The Tipping Point Resiliency Index (TPRI)

To measure overall resiliency to security concerns, respondents were given four different scenarios in which the benefits of a popular Web 2.0 service are weighed against the potential risks.

The scenarios included:

> A social network on health and wellness where users share information about their medical conditions and treatments. This network is potentially subject to unauthorized use by employers, insurance companies, and government agencies.

> A free social messaging utility that allows users to communicate and share information, photos and news about themselves or others. This utility is subject to potential marketing or advertising abuse.

> An online community for business professionals interested in volunteering their time for good causes. The community has had problems with members sharing confidential information about their employers, including financial statistics and product research.

> A corporate wiki designed to create a sense of community between employees, especially those in remote locations. The wiki has seen some employees post uncensored content, including unflattering photos and criticism of colleagues and confidential company information.

Tipping Point Resiliency Index

	United States	Brazil	Russia	China	Singapore	Sweden	Germany	Average
Social network for health and wellness								
Before incident: Will you use this?	54	73	41	31	32	46	46	46
After incident: Will you use this?	61	78	51	73	72	38	36	58
Net	-7	5	10	42	40	-8	-10	12
Free social messaging								
Before incident: Will you use this?	54	72	52	57	59	48	54	57
After incident: Will you use this?	41	52	56	34	26	30	27	38
Net	-13	-20	4	-23	-33	-18	-27	-19
Online community for social and business activities								
Before incident: Will you use this?	54	58	47	20	31	57	59	47
After incident: Will you use this?	31	50	50	13	16	32	27	31
Net	-23	-8	-3	-7	-15	-25	-32	-15
Wiki in the Workplace								
Before incident: Will you use this?	47	56	31	20	26	53	54	41
After incident: Will you use this?	40	40	33	37	31	38	20	25
Net	-7	-23	-23	6	11	12	-33	-29
Overall								
Before incident: Will you use this?	52	65	43	32	37	51	53	48
After incident: Will you use this?	43	53	49	38	38	30	29	40
Net	-9	-12	6	6	1	-21	-25	-8

*Rates = expressed as percentage × 100; Participation rate in scenario before data security incident = X; Participation rate in scenario after data security incident = Y (for those that answered affirmatively above) Resiliency score is established as the difference termed R = {Y - X}; For R > 0; resiliency is high and for R ≤ 0 resiliency is low.

Rank order on resilience measures	3	4	1	1	2	5	6	

TPRI Conclusions

From the TPRI results, we can make a few assumptions as it relates to how private enterprises should approach Web 2.0 matters.

> Different geographies have vastly different tolerance levels for security and privacy risk with Web 2.0. This implies that a single, worldwide policy on Web 2.0 usage may not be advisable for global firms looking to encourage use. Policies must be locally tailored to suit the cultural norms of a region.

> The value and personal relevance of content is critical to adoption of Web 2.0 technologies. Even in the least resilient locations (Germany and Sweden), health and wellness content greatly increased the willingness of users to accept vulnerability. But even this is subject to geographical variance.

> Resiliency is lower than average among users of Web 2.0 applications at or for work. This indicates that users understand the risks associated with revealing both personal and business information in a working environment, and the natural inclination to exercise cautions when doing souncensored content, including unflattering photos and criticism of colleagues and confidential company information.

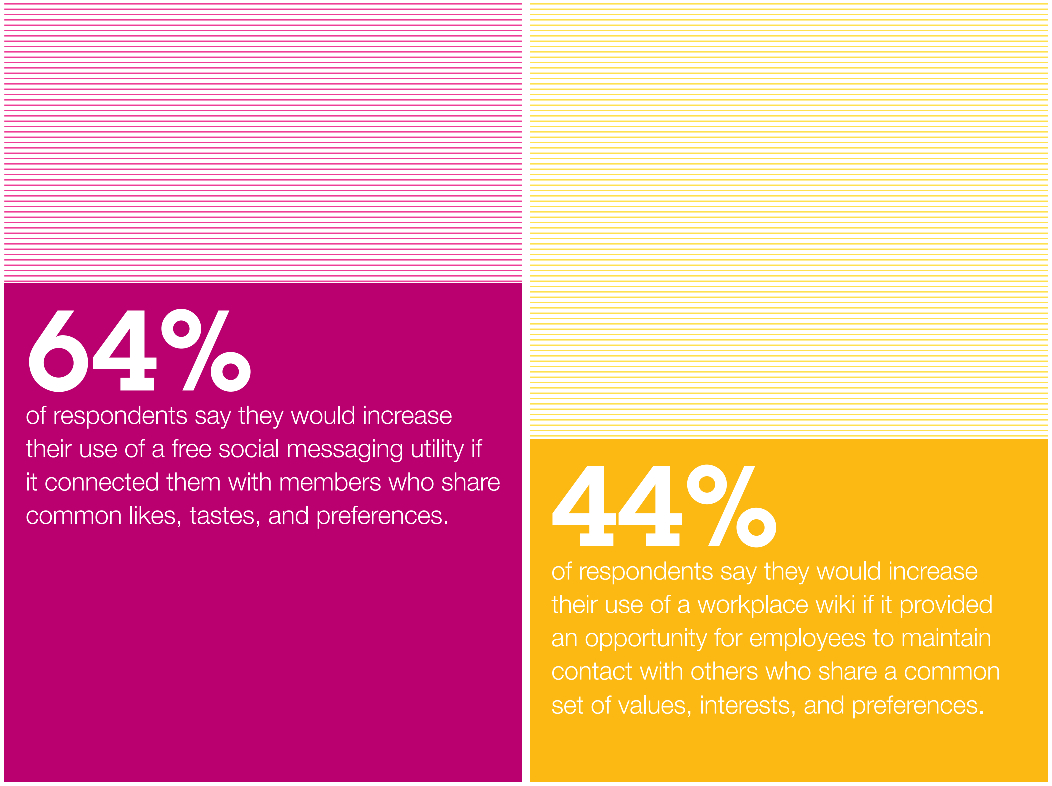
Who, What and Where

The three factors of resiliency

Based on the results of the Tipping Point Resiliency Index, and supported by various other questions from the survey, there are at least three major factors that shape an individual's resiliency to security and privacy risk when using Web 2.0 applications. These are the "Who, What, and Where" factors of community, content, and culture.

Who

A sense of **familiarity and common interests** is critical in bolstering resiliency. Respondents were more likely to increase their use of a Web 2.0 application, despite perceived security and privacy risks, if they shared thematic interests with others in the community.



64%

of respondents say they would increase their use of a free social messaging utility if it connected them with members who share common likes, tastes, and preferences.

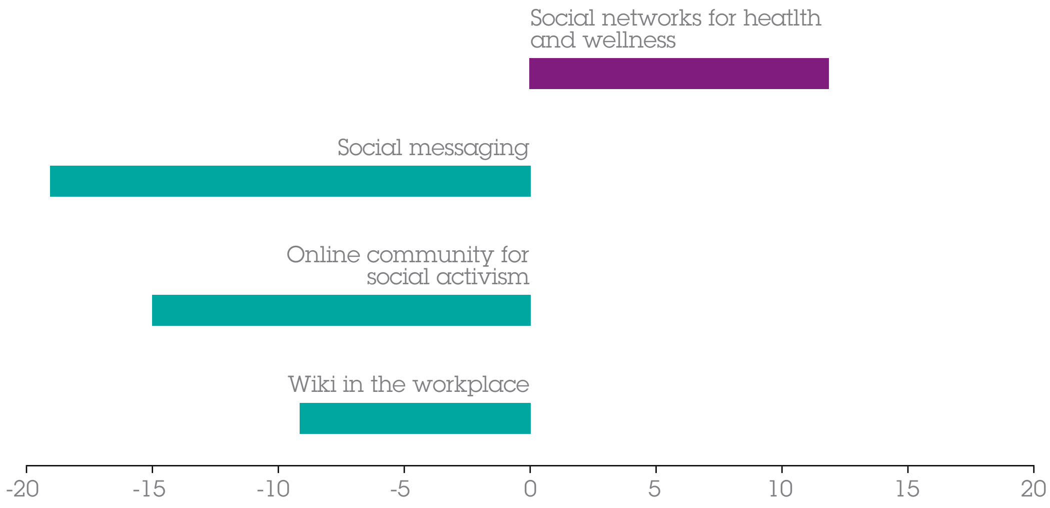
44%

of respondents say they would increase their use of a workplace wiki if it provided an opportunity for employees to maintain contact with others who share a common set of values, interests, and preferences.

What

The **type of content** a Web 2.0 application offers makes a significant difference in how committed users stay to the service, and what kind of information they are willing to divulge. Resiliency is increased by the **perceived value of the site**, and the type of information divulged is affected by the nature of the content.

Average resiliency scores



49%

of Chinese and Singaporean respondents said they use Web 2.0 applications because they believe the security of the application is adequate in protecting their personal information.

Only

7%

of Swedish and German respondents said the same.

Where

Geographical and cultural differences have a major impact on resiliency scores. In general, European Union countries have the lowest tolerance for security and privacy risk, while Asia and Russia have the highest.

Country	Resiliency Rank	Score
China	1	+6
Russia	1	+6
Singapore	2	+1
United States	3	-9
Brazil	4	-12
Sweden	5	-21
Germany	6	-25

Responsibility and Risk

Web 2.0 communities favor self-policing, transparency and control

True to the progressive, empowering nature of Web 2.0 applications themselves, users of these services have progressive, and still evolving, views on who should be responsible for ensuring their security. In many cases, respondents believe that individuals or the communities themselves should bear the responsibility for security.

In some of the more community-oriented sites on the Web, this is already happening. “In World of Warcraft, for example, players assign each other rankings based on reputation and contribution,” says Gunter Ollman, chief security strategist at IBM Internet Security Systems. “If someone insists on being disruptive and not playing by the rules, they will find themselves quickly ostracized by the group. There are even organized “vigilante” groups that will track down chronic abusers of the rules, regardless of changes in their in-game identities, and publicly post records of their behavior as a warning to others. Once you build up a bad reputation, it becomes very hard to escape it.”

But here especially, there are **significant regional differences**.

Who do you believe is most responsible for ensuring a safe Internet?

Please rank the following list from
1 = most responsible to 5 = least responsible.

	United States	Brazil	Russia	China	Singapore	Sweden	Germany	Average
Individual users	2.03	2.10	2.08	3.71	3.34	3.82	3.90	3.00
The online community as a whole	2.99	3.50	3.15	3.13	3.43	2.78	2.76	3.11
Internet service provider	4.21	4.32	4.25	3.96	3.95	4.42	4.04	4.16
Law enforcement	4.56	4.10	4.25	3.55	3.39	3.33	3.16	3.76
Government	3.42	3.71	3.44	2.22	3.18	2.79	2.55	3.04

One thing that all regions agree on is that the online communities themselves should take significant steps to protect their members. Setting standards for acceptable behavior, enforcing compliance with those standards, and implementing security tools to detect and prevent non-compliance are among the basic services users expect. And by allowing for anonymity among users, limiting the amount of personal information required to join, and developing clear and transparent policies on security and privacy, user concerns can be further assuaged.

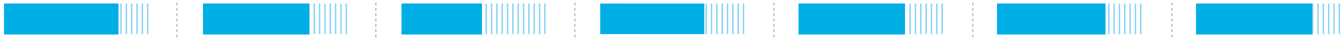
"I think that privacy is too often juxtaposed with security, and it's assumed that security means that you're giving up privacy," says Chris Kelly, Chief Privacy Officer at Facebook. "But I think you can have a great deal of control over your personal information and still maintain a secure environment. In fact, having that control can result in a more secure environment."

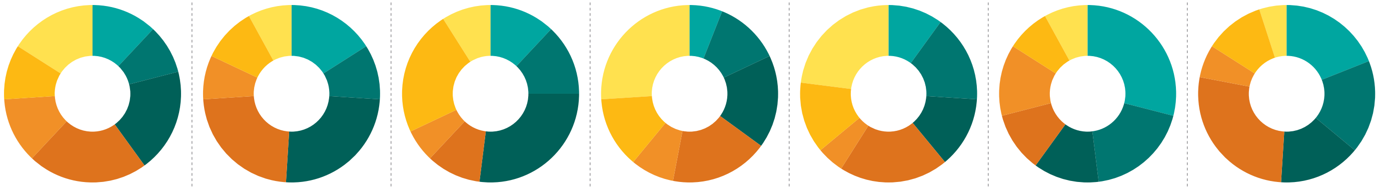
For its part, Facebook recently overhauled its security and privacy controls. In an open letter from founder Mark Zuckerberg to all 350 million users of the service, the popular social networking site added the ability to control who sees each individual piece of information on a person's profile. The open letter speaks to the kind of transparency Web 2.0 users are looking for, and the changes to the privacy settings are exemplary of the level of control users demand.

Do you believe the online community should take steps to protect its members?

🟦 Yes ▥ No

	United States	Brazil	Russia	China	Singapore	Sweden	Germany
	781 respondents	563 respondents	419 respondents	588 respondents	327 respondents	188 respondents	498 respondents
🟦 Yes / ▥ No	80% / 20%	74% / 26%	57% / 43%	73% / 27%	74% / 26%	76% / 24%	81% / 19%



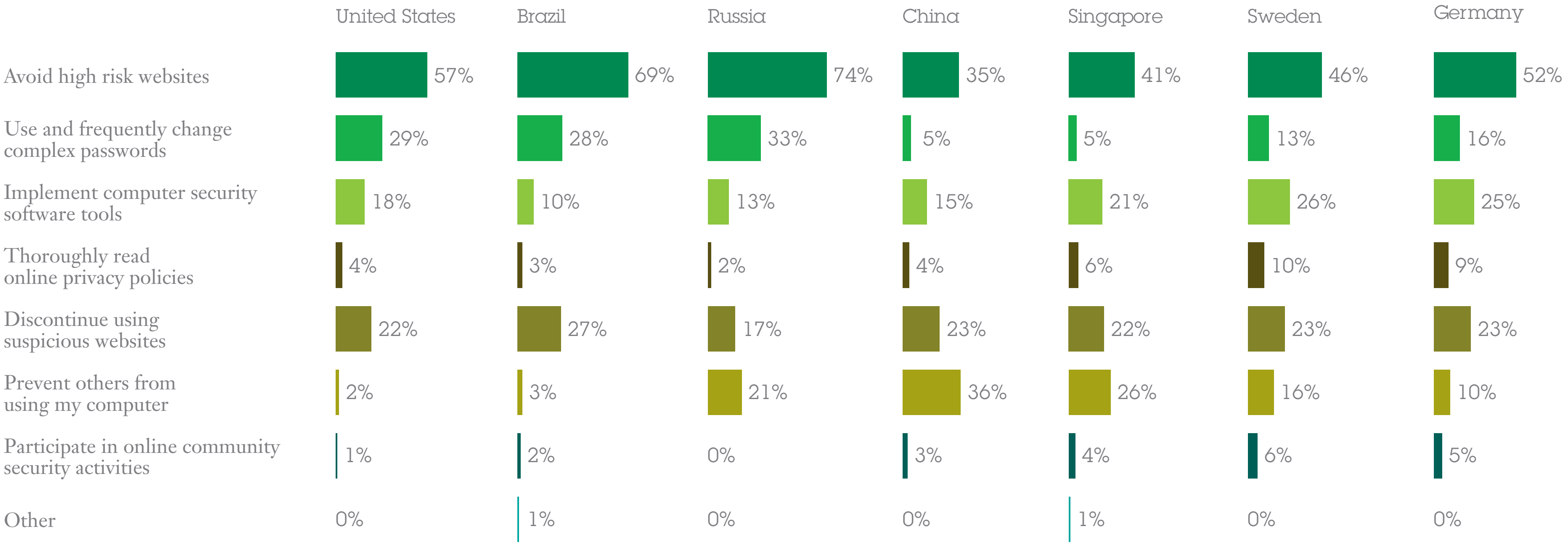


If yes, how would this work? (Top two choices).

	United States	Brazil	Russia	China	Singapore	Sweden	Germany
Set a code or standards that specifies acceptable behaviors	12%	16%	12%	6%	10%	29%	19%
Educate members about how to avoid potential harms	9%	10%	13%	12%	16%	19%	17%
Enforce compliance with acceptable standards of behavior	19%	25%	27%	17%	13%	12%	15%
Implement security tools to detect and prevent undesirable behavior	22%	23%	10%	18%	20%	11%	27%
Demand social network provider to have better safeguards in-place	12%	8%	6%	8%	5%	13%	6%
Monitor online activities to detect threats	10%	10%	23%	13%	13%	8%	11%
Work with law enforcement to police website for suspicious activity	16%	8%	9%	26%	23%	8%	5%

While it's true that Web 2.0 users are demanding control, it's not always clear that delivering that control will result in more secure online behavior. For example, there is a definite limit to what individual users are willing to do to ensure their safety and security. Users are most willing to avoid high risk or suspicious Web sites; less willing to familiarize themselves with online privacy policies or participate in community security activities.

What are you willing to do in order to ensure online safety and security?



Still, experts believe that over the long run offering users **control and transparency**, regardless of whether they take advantage of it, will create a more trusting and secure user base.

"We know that empowering people to take responsibility for their own assets is an important part of delivering security; users are part of the system and so will inevitably have a positive or negative effect on vulnerability and exposure to threats," says Sadie Creese, Director of e-Security at the University of Warwick Digital Library.

"By enabling people to take effective control over their personal information we can begin to limit the level of vulnerability they have to identity theft and associated crime. This in turn has benefits for wider society as it will help to prevent fraudulent access to corporate assets and citizen services, and play a part in fighting organized crime and terrorism."

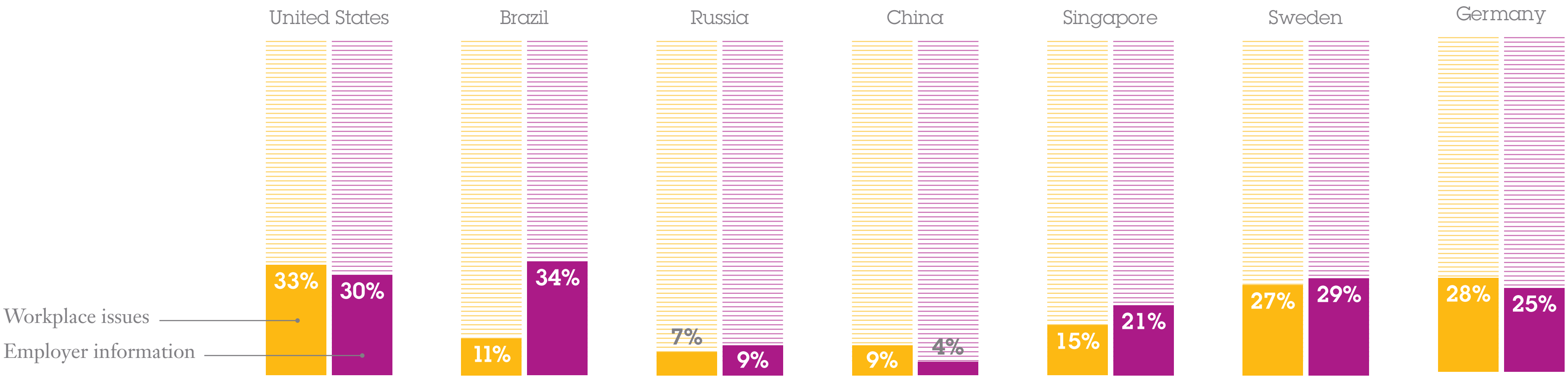
Web 2.0 and the Workplace

Sharing information, inside and outside of the office

Early on, many corporations tried to limit the use of Web 2.0 applications from within the company firewall. They feared the applications would weaken security, provide an outlet for confidential information, and drain endless hours of productive time from employees. Though those fears were not totally unfounded, most companies found that restricting Web 2.0 use among employees was neither practical nor reasonable. And since then, a combination of external and internal Web 2.0 usage has sprouted throughout corporate networks all over the world.

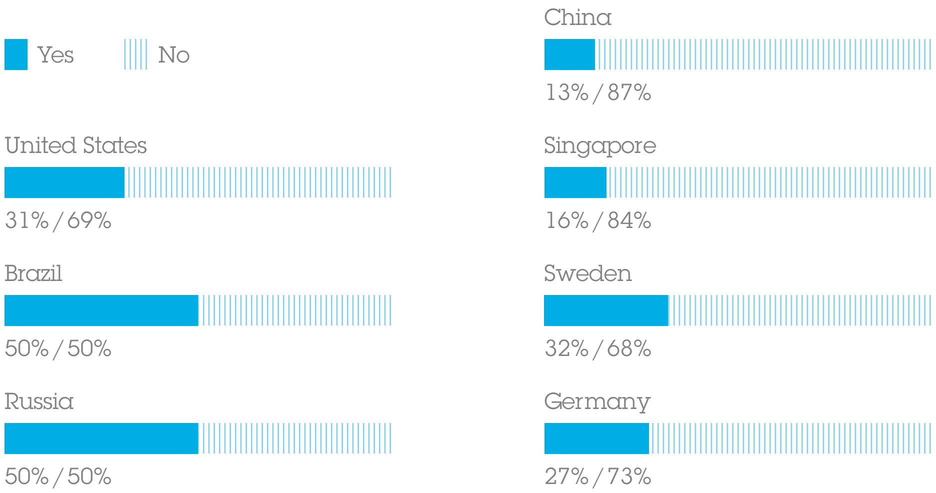
Guidelines for appropriate behavior and use of these applications within a corporate setting are still evolving. Sometimes these guidelines are set by a company; sometimes by a department manager; and sometimes they are not set at all. Some companies are embracing the spirit of Web 2.0 and allowing their employees to work collaboratively to set their own guidelines and behavioral expectations. Several years ago, IBM used a wiki develop its corporate blogging policy, soliciting input from all of its 400,000 employees. The company has since extended the same approach to other Web 2.0 technologies.

Global respondents that are willing to share workplace issues or employer information on a social network community



Many employers have come to see the value of Web 2.0 applications in the workplace, both for the purposes of working and communicating with the outside world. And common sense has led most Web 2.0 users to observe the same rules of the road they would in any other circumstance. In general, that means a healthy dose of caution, especially when posting information on an external site.

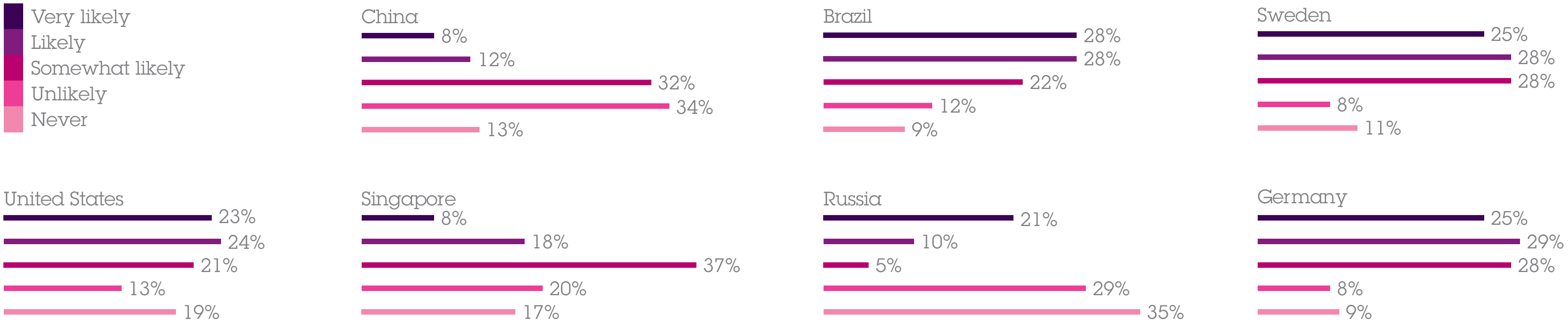
Would you still consider using a social network knowing that it creates a risk to the security of confidential data about your company?



When it comes to using Web 2.0 applications that are specifically designed for the corporate setting, respondents are circumspect. In general, employees are willing to use a wiki that enables them to share information about themselves and their work.

The list of reasons why an employee would use a workplace wiki is long and varied. But across the board, respondents agreed that relevant and timely information about the company in which they work was a strong incentive for using the application. Other factors that increased use were the development of a sense of community and the ability to control the content that identifies them.

How likely would you be to use a wiki that enables you to share information about yourself and your work?



Interestingly, the ability to post content anonymously ranked high among these responses. But in other survey questions, respondents indicated they are likely to willingly share personal information about themselves. This demonstrates that users of Web 2.0 applications appreciate and value the option to remain anonymous, even if they choose not to exercise it. It increases their trust in the provider of the service.

The following is a list of possible factors that may affect your use of this wiki. Adjacent response = increase use

	United States	Brazil	Russia	China	Singapore	Sweden	Germany
The wiki provides relevant and timely information about the organization.	51%	66%	59%	43%	46%	69%	63%
The wiki provides opportunities for employees to organize and unite on critical issues.	40%	48%	49%	4%	18%	57%	56%
The wiki provides an opportunity for employees to maintain contact with others who share a common set of values, interests and preferences.	62%	59%	41%	21%	26%	68%	51%
The wiki provides opportunities to freely communicate issues and concerns with the organization's management.	40%	53%	17%	5%	25%	59%	58%
The company provides clear disclosure about posting content that may make others feel uncomfortable.	43%	22%	20%	14%	18%	40%	44%

(continued)

	United States	Brazil	Russia	China	Singapore	Sweden	Germany
The company ensures anonymity wherein the employee's identity cannot be determined when he or she posted content to the wiki.	59%	49%	50%	50%	54%	62%	59%
The company implements strict authentication over who is able to post content to the wiki.	52%	60%	63%	71%	57%	43%	50%
The company sets standards about the posting of business information.	39%	24%	20%	33%	37%	57%	50%
The company censors all content before posting to the wiki.	25%	10%	14%	47%	40%	38%	40%
Employees have the ability to control, modify or delete any content that identifies them.	69%	77%	50%	20%	36%	55%	65%
The community of wiki users set standards of acceptable behavior.	36%	25%	20%	30%	35%	52%	53%
The community of wiki users establishes a governance body to hear complaints and enforce standards.	38%	19%	15%	48%	33%	38%	43%
The community of wiki users establishes an employee group to censor content before posting.	38%	16%	22%	55%	49%	39%	39%
Goverment sets regulations that restrict companies from using wikis that may reveal an employee's personal information	40%	16%	10%	39%	45%	39%	31%

The role that an employer plays in engendering trust and respect among participants in these applications is critical of they are to be of value to the overall operation. For example, when IBM sought to embrace blogging across the company in 2005, it set up a wiki and allowed IBMers to develop their own guidelines. Since then the wiki has expanded to include all social computing. But the guidelines that continue to evolve invariably follow well understood, long-standing corporate policies and good-old fashioned common sense.

“Employers can do a lot by educating employees—keeping the issues on the proverbial radar screen,” says Harriet Pearson, vice president, regulatory policy and chief privacy officer at IBM. “But even the best-intentioned employees sometimes don’t practice good security behavior. So we recommend that employers architect corporate policies and an environment that makes secure and trusted behavior the obvious choice.”

Conclusions

The success and longevity of Web 2.0 is no longer in question; it is a model that will be with us for a long time to come. But the extent to which a Web 2.0 application can foster collaboration and innovation within and between companies depends on the security comfort-level of its user base.

To address this effectively, organizations should consider the cultural and regional expectations of privacy and craft policies that reflect them. They should employ Web 2.0 services only where they will deliver tangible value to end users. And they should give employees an active role in both creating usage guidelines and enforcing them.

Using the insights generated from this study, developers and employers can build sensible security provisions and maximize the value of their Web 2.0 applications. And maybe even pave the way for the next evolutionary step of the World Wide Web.

About the Ponemon Institute

Ponemon Institute conducts independent research on privacy, data protection and information security policy. Our goal is to enable organizations in both the private and public sectors to have a clearer understanding of the trends in practices, perceptions and potential threats that will affect the collection, management and safeguarding of personal and confidential information about individuals and organizations. Ponemon Institute research informs organizations on how to improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise.

About the GIO

Over five years ago, IBM launched a unique experiment in exploration, collaboration and innovation: the Global Innovation Outlook (GIO). During its evolution, we've convened hundreds of thought leaders, policymakers, business executives, university researchers and representatives from non-profit organizations. We've explored topics as varied and important as healthcare, energy and the environment, economic development in Africa, and the future of the world's water resources. We've shared the results of our exploration and analysis through reports and studies, brokered new relationships, and launched dozens of collaborative initiatives among GIO participants.

The idea of the GIO emerged from a central insight and belief about 21st century innovation, one that was enthusiastically validated across every session we held in its inaugural year: innovation is no longer a solitary exercise. Instead innovation will increasingly need to be open, intensely collaborative, multi-disciplinary and global in its reach and impact. Today this belief pervades just about all IBM interactions. It is clearly visible in our thinking about building a Smarter Planet, and our implicit invitation for like-minded people around the world to join us in this endeavor.

Engage with IBM at any level today, and you will witness this belief in action, as well as the culture it engenders. It's how we do business, how we get things done—how we help make the world work better. So in a sense, the GIO itself is no longer necessary as a standalone program, and so we will no longer be conducting separate GIO deep dives, roundtables or forums as such. We will, however, continue to support and cultivate the communities essential to the spirit of the GIO, including the GIO Facebook and LinkedIn communities, so that GIO alumni can contact each other and IBM as often as they wish. GIO reports and other collateral material will also remain available. And the GIO blog archives will continue to be hosted at http://www.gio.typepad.com/.

If we've been fortunate enough to have you participate in one of our GIO sessions, we trust that the people you've met and the topics you've discussed have been extremely valuable to you and your organization. And we encourage you to continue to engage with us at IBM, as well as your fellow GIO Alumni.

Appendix A—Audited Findings

Countries	United States	Brazil	Russian Federation	People's Republic of China	Singapore	Sweden	Germany
Abbreviated Country	US	BZ	RF	CH	SG	SW	DE
Panel	15,998	14,083	11,620	19,001	6,780	3,512	8,049
Sample	781	563	419	588	327	188	498
Response	4.9%	4.0%	3.6%	3.1%	4.8%	5.4%	6.2%

Do you use social networks, social messaging, blogs, wikis, or other Web 2.0 tools on the Internet?

	US	BZ	RF	CH	SG	SW	DE
Yes	586 (75%)	418 (74%)	339 (81%)	183 (31%)	235 (72%)	155 (82%)	400 (80%)
No (Stop)	195 (25%)	145 (26%)	80 (19%)	405 (69%)	92 (28%)	33 (18%)	98 (20%)
Total	781	563	419	588	327	188	498

Appendix A—Audited Findings

Countries	United States	Brazil	Russian Federation	People's Republic of China	Singapore	Sweden	Germany
Abbreviated Country	US	BZ	RF	CH	SG	SW	DE
Panel	15,998	14,083	11,620	19,001	6,780	3,512	8,049
Sample	781	563	419	588	327	188	498
Response	4.9%	4.0%	3.6%	3.1%	4.8%	5.4%	6.2%

If yes, how are using these Web 2.0 applications? Please select all that apply.

	US	BZ	RF	CH	SG	SW	DE
Performing search	418	356	250	85	185	119	356
Obtaining news and information	509	391	227	53	160	135	367
Participating in a social network	290	187	187	52	111	80	239
Using social messaging tools	248	150	146	31	105	75	201
Browsing or shopping	552	382	244	89	201	133	353
Banking or paying bills	398	56	23	0	5	17	50
None of the above (Stop)	24	18	24	40	29	15	44
Total	781	563	419	588	327	188	498

Appendix B—Web 2.0 Scenarios

Social network on health & wellness

A new social network has been introduced to provide information sharing opportunities about healthy living, medical treatments, clinical trials and health care insurance. This social network provides opportunities to communicate freely with others who have similar medical conditions.

The network claims to benefit individuals by helping them make better decisions about their health care options. The network also offers medical advice on such sensitive health concerns as depression, obesity and addictive behaviors and encourages individuals to share their healthrelated experiences in overcoming these problems.

Incident

Users of this social network reap many benefits including up-to-date facts about new medical treatments, discounts on pharmaceutical products, a mechanism for obtaining free and unbiased medical advice, and the ability to communicate with others who have similar medical issues or general health conditions.

Some of the users of this social network suspected that personal information about their health conditions has leaked out to employers, insurance companies, government agencies and others. An investigation by the social networking provider revealed that unauthorized users infiltrated the online community posing as members or health care providers. The investigation established that these unauthorized users accessed and obtained sensitive health information.